PUBLISHED DOCUMENT

PD ISO/TR 18307:2001

Health informatics — Interoperability and compatibility in messaging and communication standards — Key characteristics

ICS 35.240.80

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

British Standards

Full document details: PD ISO/TR 18307:2001

National foreword

This Published Document reproduces verbatim ISO/TR 18307:2001.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics, which has the responsibility to:

— aid enquirers to understand the text;

— present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;

— monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international publications referred to in this document may be found in the *BSI Catalogue* under the section entitled "International Standards Correspondence Index", or by using the "Search" facility of the *BSI Electronic Catalogue* or of British Standard Online.

This Published Document, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Policy and Strategy Committee on 10 October 2002

Summary of pages

This document comprises a front cover, an inside front cover, the ISO/TR title page, pages ii to v, a blank page, pages 1 to 93 and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

© BSI 10 October 2002

ISBN 0 580 40542 7

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

TECHNICAL REPORT

ISO/TR 18307

First edition
2001-12-15

Health informatics — Interoperability and compatibility in messaging and communication standards — Key characteristics

Informatique de santé —Interoperabilité et compatibilité avec les normes de messagerie et de communication — Caractéristiques

Reference number
ISO/TR 18307:2001(E)

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

Contents

Page

Foreword v

1 Scope 1

2 References 1

3 Terms and definitions 1

4 Abbreviated terms 21

5 Trust Constituency 23

6 Principles and objectives 24
6.1 Ensured Trust 24
6.2 Trust Constituency 25
6.3 Health record rights 25
6.4 Health record obligations 26
6.5 Health record composition 26
6.6 Healthcare parties and their accountable actions 27
6.7 Healthcare agents and their accountable actions 27
6.8 Scope of accountability, Unit of accountability 27
6.9 Authentication 28
6.10 Auditability 28
6.11 Chain of trust 28
6.12 Faithfulness, permanence, persistence and indelibility 28
6.13 Data definition, Data registry 28
6.14 Data integrity 29
6.15 Completeness and continuity 29

7 Key characteristics (KC) 29
7.1 Identifiable information 29
7.2 Architectural basis 30
7.3 Master files 33
7.4 Master registries 37
7.5 Electronic records 40
7.6 Record chronology, continuity, completeness 42
7.7 Authentication, non-repudiation services 43
7.8 Digital signature, Public key infrastructure 44
7.9 Audit 44
7.10 Permanence, persistence, indelibility 45
7.11 On-Line Transaction Processing (OLTP) 45
7.12 On-Line Analytical Processing (OLAP) 46
7.13 Fault tolerance 46
7.14 Data synchrony 46
7.15 Time synchrony 47
7.16 Trusted end-to-end information flows 47
7.17 Disclosure, Export 49
7.18 Prospective services 50
7.19 Work flow 52
7.20 Concurrent status, Records 53
7.21 Retrospective status, Records 54
7.22 Personal healthcare professional services 54
7.23 Data integrity 55
7.24 Protocols: Care plans, Critical paths 56
7.25 Problem lists 56
7.26 Decision support 56

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

7.27 Surveillance, Metrics and Analysis 57
7.28 Communications infrastructure 58
7.29 Multiple person linkage 58
7.30 Healthcare professional — Subject of care linkage 59
7.31 Localization, Local authority 59
7.32 User environments 60
7.33 Version management 60
7.34 Inter-application interoperability 60
7.35 Change scale (Scalability) 62
7.36 Validation 62

8 Principles and objectives enabled by key characteristics 63

Annex A Exercise to validate the key characteristics set out in this technical report 69

Annex B RM-ODP viewpoints 89

Annex C RM-ODP enterprise viewpoint 90

Annex D RC-ODP architecture — Enterprise language 91

Bibliography 92

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard (“state of the art”, for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this Technical Report may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 18307 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

Health informatics — Interoperability and compatibility in messaging and communication standards — Key characteristics

1 Scope

This Technical Report describes a set of key characteristics to achieve interoperability and compatibility in trusted health information interchange between communicant application systems.

The key characteristics describe inter-application interoperability needs of the healthcare community, in particular the subject of care, the healthcare professional/caregiver, the healthcare provider organization, its business units and the integrated delivery network.

The key characteristics offer criteria for standards developers and implementers of standards for messaging and communications in the healthcare domain and provide a guide for software developers and vendors, healthcare providers and end users.

2 References

ISO/IEC Guide:1996, Guide 2: definition 3.2

ISO 2382-4, *Information technology — Vocabulary — Part 4: Organization of data*

ISO 6523-1:1998, *Information technology — Structure for the identification of organizations and organization parts — Part 1: Identification of organization identification schemes*

ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

ISO/IEC 10746-2:1996, *Information technology — Open Distributed Processing — Reference Model: Foundations*

ISO/IEC 10746-3:1996, *Information technology — Open Distributed Processing — Reference Model: Architecture*

ISO/IEC 10746-4:1998, *Information technology — Open Distributed Processing — Reference Model: Architectural Semantics*

ISO/IEC 15408-1:1999, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

3 Terms and definitions

3.1
access
ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource

[HIPAA]

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

provision of an opportunity to approach, inspect, review, make use of data or information

[CPRI]

specific type of interaction between a subject and an object that results in the flow of information from one to the other

[GCST]

3.2
access control
means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways

[ISO/IEC 2382-8]

prevention of an unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner

[ISO 7498-2]

policies and procedures preventing access by those who are not authorized to have it

[IOM]

3.3
access level
level associated with an individual who may be accessing information (e.g. a clearance level)…, the information which may be accessed (e.g. a classification level)

[HIPAA]

3.4
accountability
property that ensures that the actions of an entity can be traced uniquely to the entity

[ISO 7498-2]

concept that individual persons or entities can be held responsible for specified actions

[NRC]

obligation to disclose periodically, in adequate detail and consistent form, to all directly and indirectly responsible or properly interested parties, the purposes, principles, procedures, relationships, results, incomes and expenditures involved in any activity, enterprise, or assignment so that they can be evaluated by the interested parties

[JCAHO]

3.5
actor
⟨with respect to an action⟩ an enterprise object (or entity) that participates in the action

[ISO/IEC 15414]

3.6
agent
enterprise object (or entity) that has been delegated (authority, a function, etc.) by and acts for another (in exercising the authority, performing the function, etc.)

[ISO/IEC 15414]

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

3.7
aggregate
aggregation
to combine standardized data and information

[JCAHO]

3.8
algorithm
algorithmic
series of steps for addressing a specific issue

[JCAHO]

3.9
application
identifiable computer running a software process

NOTE 1 In this context, it may be any software process used in healthcare information systems including those without any direct role in treatment or diagnosis.

NOTE 2 In some jurisdictions, including software processes may be regulated medical devices.

3.10
architecture
set of principles on which the logical structure and interrelationships to an organization and business context are based

NOTE Software architecture is the result of software design activity.

3.11
archived (records)
archival (records)
⟨healthcare⟩ data saved for later reference or use, possibly off-line

[COACH]

3.12
assurance
grounds for confidence, surety, certitude

grounds for confidence that an entity meets its security objectives

[ISO/IEC 15408:1999]

development, documentation, testing, procedural and operational activities carried out to ensure a system's security services do in fact provide the claimed level of protection

[OMG 97]

3.13
asymmetric cryptographic algorithm
algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ

[ISO 10181-1]

3.14
audit control
mechanisms employed to record and examine system activity

[HIPAA]

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

3.15
audit trail
record of the resources which were accessed and/or used by whom

[ISO 7498-2]

documentary evidence of monitoring each operation (of healthcare parties) on health information

[NRC]

chronological record of system activities that is sufficient to enable the reconstruction, reviewing and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results

[GCST]

3.16
authentication of health record entries
process used to verify that an entry is complete, accurate and final

[JCAHO]

3.17
authentication
providing assurance regarding the identity of a subject (author) or object (information)

[ASTM E1762]

3.18
authentication (data)
verification of the integrity of data that have been stored, transmitted or otherwise exposed to possible unauthorized modification

[GCST]

3.19
authentication (data source)
corroboration that the source of data received is as claimed

[ISO 7498-2]

3.20
authentication (user)
provision of assurance of the claimed identity of an entity

[ISO/IEC 10181-2]

3.21
authorize
authorization
granting of rights, which includes granting of access based on access rights

[ISO 7498-2]

prescription that a particular behaviour must not be prevented

[ISO/IEC 15414]

3.22
authorized user
user who may, in accordance with the Security Policy, perform an operation

[ISO/IEC 15408:1999]

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001

3.23
availability
property of being accessible and useable upon demand by an authorized entity

[ISO 7498-2]

prevention of the unauthorized withholding of information or resources

[ITSEC]

3.24
biometric
biometrics
use of specific attributes that reflect unique personal characteristics, such as a fingerprint, an eye blood-vessel print, or a voice print, to validate the identity of entities

[ISO/IEC 2382-08]

3.25
business unit
discrete and accountable function or sub-function within an organization

NOTE For example, a business unit includes a department, service or speciality of a healthcare provider organization.

3.26
care
provision of accommodations, comfort and treatment to an individual subject of care (patient), also implying responsibility for safety

[JCAHO]

3.27
caregiver
cf. **healthcare professional** (3.76)

3.28
care plan
cf. **critical path** (3.47)

3.29
certificate
public key certificate
user certificate
public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it

[ISO 9594-8]

agreement that binds a user's name to a public key, signed by a trusted issuer

[NRC]

NOTE A framework for the use of public key certificates is defined in CCITT Standard X.509.

3.30
certificate policy
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

[X.509]

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

3.31
certification
procedure by which a third party gives assurance that all or part of a data processing system conforms to security requirements

[ISO/IEC 2382-08]

administrative act of approving a system for use in a particular application

[NRC]

3.32
certification authority
CA
certificate issuer
authority trusted by one or more relying parties to create and assign certificates

[ISO 9594-8]

NOTE Optionally the certification authority may create the relying parties' keys.

3.33
ciphertext
data produced through the use of encipherment; the semantic content of the resulting content is not available

[ISO 7498-2]

3.34
classification level
security level of information

[NSC]

3.35
clearance level
permission granted to an individual to access information at or below a particular security level

[ISO/IEC 2382-08]

3.36
clinical information
information about a subject of care, relevant to the health or treatment of that subject of care, that is recorded by or on behalf of a healthcare person

[CEN ENV 1613:1995]

data/information related to the health and healthcare of an individual collected from or about an individual receiving healthcare services: includes a caregiver's objective measurement or subjective evaluation of a patient's physical or mental state of health; descriptions of an individual's health history and family health history; diagnostic studies; decision rationale; descriptions of procedures performed; findings; therapeutic interventions; medication prescribed; description of responses to treatment; prognostic statements; and descriptions of socio-economic and environmental factors related to the patient's health

[ASTM E1769, CPRI]

3.37
code set
any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes

[HIPAA]

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001

3.38
coding scheme
collection of rules that maps the elements of one set on to the elements of a second set

[ISO/IEC 7826]

3.39
complete health record
final, assembled and authenticated, health record for an individual

(health) record is complete when a) its contents reflect the diagnosis, results of diagnostic tests, therapy rendered, condition and progress (of the subject of care), and condition (of the subject of care) at discharge, and b) its contents, including any required clinical résumé or final progress notes, are assembled and authenticated, and all final diagnoses and any complications are recorded without use of symbols or abbreviations

[JCAHO]

3.40
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[ISO 7498-2]

condition in which information is shared or released in a controlled manner

[NRC]

prevention of the unauthorized disclosure of information

[ITSEC]

restriction of access to data and information to individuals who have a need, a reason and permission for access

[JCAHO]

status accorded to data or information indicating that it is sensitive for some reason, and that therefore it needs to be protected against theft or improper use and must be disseminated only to individuals or organizations authorized to have it

[OTA]

3.41
consent
voluntary agreement with what is being done or proposed (express or implied)

[CIHI]

communication process between the caregiver and the (subject of care), and which may refer to consent for treatment, special procedures, release of information and advance directives [which give instructions regarding the (subject of care's) wishes in special medical situations]

[CPRI]

3.42
continuity of care
component of patient care quality consisting of the degree to which the care needed by a patient is coordinated among practitioners and across organizations and time

[JCAHO]

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

3.43
constituency
class of persons served in common

NOTE A group of individuals and/or organizations with explicit common interests and who may elect or otherwise designate agents or delegates to represent such interests.

3.44
credentials (for identity)
data that are transferred to establish the claimed identity of an entity

[ISO/IEC 2382-08]

3.45
credentials (for healthcare practice)
documented evidence of (a healthcare professional's) licensure, education, training, experience, or other qualifications

[JCAHO]

3.46
criteria
expected level(s) of achievement, or specifications against which performance can be assessed

[JCAHO]

3.47
critical path(s)
care plan(s)
clinical pathway(s)
plan, based on data gathered during (subject of care) assessment, that identifies the care needs, lists the strategy for providing services to meet those needs, documents treatment goals and objectives, outlines the criteria for terminating specified interventions, and documents the (subject of care's) progress in meeting specified goals and objectives

[JCAHO]

3.48
cryptography
discipline, which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

[ISO 7498-2]

art of keeping data secret, primarily through the use of mathematical or logical functions that transform intelligible data into seemingly unintelligible data and back again

[NRC]

3.49
cryptographic algorithm
cipher
method for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

[ISO 7498-2]

3.50
data attribute, element or item
single unit of data that in a certain context is considered indivisible

[CEN ENV 13606-4]

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001

3.51
data reliability
stability, repeatability, or precision of the data

[JCAHO]

3.52
data transmission
data transmittal
sending of data or information from one location to another location

[JCAHO]

exchange of data between person and program, or program and program, when the sender and receiver are remote from each other

[CPRI]

3.53
data validity
verification of correctness (reflecting the true situation)

[JCAHO]

3.54
decision support
(typically) electronic system designed to aid healthcare professionals make clinical decisions

3.55
decipherment
decryption
process of obtaining, from a ciphertext, the original corresponding data

[ISO/IEC 2382-8]

process of decoding a message so that its meaning becomes obvious

[OTA]

3.56
de-identified data
data resulting from personally identifiable information after the process of removing or altering one or more attributes so that the (direct or indirect) identification of the relevant person without knowledge of the initial information is either impossible or requires an unreasonable amount of time and manpower

[MEDSEC]

3.57
delegate
to give (authority, function, etc.) to another

[ISO/IEC 15414]

3.58
device
identifiable computer controlled apparatus or instrument that is the holder of a private encipherment key

NOTE This includes the class of regulated medical devices that meet the above definition. Device in this context is any device used in healthcare information systems including those without any direct role in treatment or diagnosis.

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

3.59
digital signature
data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

[ISO 7498-2]

electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified

[HIPAA]

NOTE This term is usually reserved for digital values or checksums calculated using asymmetric techniques, where only the originator of the message can generate the digital signature but many people can verify it.

3.60
disclosure (of health information)
release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information

[HIPAA]

release of information to third parties within or outside the healthcare provider organization from an individual's (health) record with or without the consent of the individual to whom the record pertains

[CPRI]

3.61
documentation
process of recording information in the (health) record

[JCAHO]

3.62
effectiveness (of care)
degree to which the care is provided in the correct manner, given the current state of knowledge, to achieve the desired or projected outcome for the (subject of care)

[JCAHO]

3.63
electronic health record
EHR
electronic healthcare record
ECHR
health record concerning the subject of care in computer-readable form

[CEN ENV13606-1]

3.64
encipherment
encryption
cryptographic transformation of data (see cryptography) to produce ciphertext

[ISO 7498-2]

process of encoding a message so that its meaning is not obvious

[OTA]

3.65
episode of care
identifiable grouping of healthcare related activity characterized by the entity relationship between the subject of care and a healthcare provider, such a grouping determined by the healthcare provider

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001

3.66
firewall
computer system providing an isolation layer between a private network security domain and a public untrusted network

[CIHI]

3.67
health information
any information, whether oral or recorded in any form or medium, that a) is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearing-house; and b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual

[HIPAA]

3.68
health record
healthcare record
account compiled [by healthcare parties (physicians and other healthcare professionals)] of a variety of (subject of care) health information, such as the (subject of care's) assessment findings, treatment details and progress notes

[JCAHO]

3.69
health record entry
healthcare record entry
dataset, suitably attributed, which forms part of, or a whole, contribution to a health(care) record at one place and time

[CEN ENV 13606-2]

3.70
healthcare
care, services, or supplies related to the health of an individual

[HIPAA]

NOTE Includes any: a) preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, counselling, service, or procedure with respect to the physical or mental condition, or functional status, of a patient or affecting the structure or function of the body; b) sale or dispensing of a drug, device, equipment, or other item pursuant to a prescription; or c) procurement or banking of blood, sperm, organs, or any other tissue for administration to patients.

3.71
healthcare agent
medical devices (e.g. instruments, monitors) and software (e.g. applications, components) which: a) perform a role in the provision of healthcare services; and/or b) are accountable for actions related to, and/or ascribed in, the health record

[CEN ENV12265, modified]

3.72
healthcare data
data which are input, stored, processed or output by the automated information system which support the clinical and business functions of a healthcare organization; these data may relate to person identifiable records or may be part of an administrative system where persons are not identified

[HL7]

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

3.73
healthcare informatics
scientific discipline that is concerned with the cognitive, information processing and communication tasks of healthcare practice, education and research, including the information science and technology to support these tasks

[Directory of the European Standardization Requirements for Healthcare Informatics and Telematics v2.1, 1994]

3.74
healthcare organization
generic term used to describe many types of organizations that provide healthcare services

[JCAHO]

3.75
healthcare party
individuals, organizations or business units, including: a) subjects of care (patients, health plan members); b) those involved in the direct or indirect provision of healthcare services to an individual or to a population; and/or c) those accountable for actions related to, and/or ascribed in, the health record

[CEN ENV 1613:1995, modified]

3.76
healthcare professional
person that is authorized by a nationally recognized body to be qualified to perform certain health services

individual who is entrusted with the direct or indirect provision of defined healthcare services to an individual subject of care or to populations

[CEN ENV 1613: 1995]

NOTE 1 The types of registering or accrediting bodies differ in different countries and for different professions. Nationally recognized bodies include local or regional governmental agencies, independent professional associations and other formally and nationally recognized organizations. They may be exclusive or non-exclusive in their territory.

NOTE 2 Examples of health professionals are physicians, registered nurses and pharmacists.

3.77
healthcare provider
healthcare organization or healthcare professional responsible for the provision of healthcare to a subject of care or to a population

[CEN 13940:2000]

3.78
health plan
individual or group plan that provides, or pays the cost of, medical care

[HIPAA]

3.79
identifier
piece of information used to claim an identity, before a potential corroboration by a corresponding authenticator

[CEN ENV 13608-1]

3.80
indelible
indelibility
impossible to remove or erase, permanent

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001

3.81
indicator (of performance)
measure used to determine over time, (an organization's) performance of functions, processes and outcomes

[JCAHO]

3.82
individually identifiable health information
any information, including demographic information collected from an individual, that a) is created or received by a healthcare provider, health plan employer, or healthcare clearing-house; and b) relates to the past, present or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual, and i) identifies the individual, or ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual

[HIPAA]

3.83
information
interpreted set(s) of data that can assist in decision making

[JCAHO]

data to which meaning is assigned, according to context and assumed conventions

[NSC]

3.84
in-patient
subject of care who is admitted to a healthcare organization for an overnight stay, in order to receive healthcare

3.85
integrity (data)
property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2]

accuracy, consistency and completeness of data

[JCAHO]

3.86
integrity (message)
proof that the message content has not altered, deliberately or accidentally in any way, during transmission

[ISO/IEC 7498-2]

3.87
interface
process that permits the flow of data from one system to another in a structured manner

3.88
interoperability
with regard to a specific task is said to exist between two applications when one application can accept data from the other and perform the task in an appropriate and satisfactory manner (as judged by the user of the receiving system) without the need for extra operator intervention

[CEN]

ability of software and hardware on multiple machines from multiple vendors to communicate; ability of a system to use the parts or equipment of another system

[HL7 Security SIG]

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

3.89
key
sequence of symbols that controls the operations of encipherment and decipherment

[ISO 7498-2]

3.90
key management
generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy

[ISO 7498-2]

3.91
longitudinal or lifetime personal health record
permanent, coordinated record of significant information, in chronological sequence; it may include all historical data collected or be retrieved as a user designated synopsis of significant demographic, genetic, clinical and environmental facts and events maintained within an automated system

[ASTM E1384]

3.92
master file
dataset containing definitional entries in common across system, business units and, in some cases, organizational boundaries

NOTE For example, master files may include data group and attribute definitions, security policy and domain definitions, security classification and clearance definitions, healthcare service definitions, care protocol definitions.

3.93
master patient index
MPI
index within a given healthcare organization which serves as a directory to patients (subjects of care)

[CPRI]

3.94
measure
collect quantifiable data about a function or process

[JCAHO]

3.95
message
logically ordered dataset designed to communicate essential information between systems

3.96
need-to-know
legitimate requirement of a prospective recipient of data to know, to access, or to possess any sensitive information represented by these data

[ISO/IEC 2382-08]

users should have access only to the data he or she needs to perform a particular function

[HIPAA]

3.97
network
electronic data transmission facility which can comprise of just a point-to-point wire link between two devices, or a complex arrangement of transmission lines

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001

3.98
non-repudiation (of origin, of submission, of receipt)
service that provides proof of the integrity and origin of data (both in an unforgeable relationship) which can be verified by any party

[ASTM]

proof (to a third party) that only the signer could have created a signature; basis of legal recognition of digital signatures

[ASTM E1762]

provision of evidence which will prevent a participant in an action from convincingly denying his/her responsibility for the action

[OMG]

3.99
object
identifiable, encapsulated entity that provides one or more services

[OMG]

3.100
organization
unique framework of authority within which a person or persons act, or are designated to act towards the same purpose

[ISO 6523:1984]

3.101
outcome
result of the performance (or non-performance) of a function or process(es)

[JCAHO]

3.102
out-patient
subject of care whose episode of care in a healthcare organization does not require an overnight (or less than 24 hour) stay in that same organization

3.103
party
object modelling a natural person or any other entity considered to have the same rights, powers and duties of a natural person

[ISO/IEC 15414]

3.104
patient
cf. **subject of care**

3.105
patient assessment
systematic collection and review of patient-specific data

[JCAHO]

3.106
patient reassessment
ongoing data collection that begins on initial assessment, comparing the most recent data with the data collected on the previous assessment

[JCAHO]

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

3.107
password
confidential authentication information composed of a string of characters

[ISO 7498-2]

sequence that an individual presents to a systems for purposes of authentication

[NRC]

3.108
payment guarantor
individual or organization responsible for the total or partial reimbursement or payment for the provision of healthcare services

[CEN ENV 13607]

3.109
performance
way in which an individual, group or organization carries out or accomplishes its important functions and processes

[JCAHO]

execution, accomplishment, fulfillment; operation or functioning, usually with regard to effectiveness

[Webster's New World Dictionary]

3.110
performance measure
measure, such as a standard or indicator, used to assess the performance of a function or process of any organization

quantification of processes and outcomes using one or more dimensions of performance, such as timeliness or availability

[JCAHO]

3.111
persistent
persistence
enduring

existing or remaining in the same state for an indefinitely long time

3.112
personal health information
any information that concerns a person's health, medical history, medical treatment or genetic characteristics in a form that enables the person to be identified

[MEDSEC]

3.113
personal information
any information relating to an identified or identifiable natural person

[EU Directive 95/46/EC, MEDSEC]

3.114
policies and procedures (for clinical care)
formal, approved description of how a governance, management of clinical care process is defined, organized and carried out

[JCAHO]

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001

3.115
policy
set of rules related to a particular purpose; a rule can be expressed as an obligation, an authorization, a permission or a prohibition

[ISO/IEC 15414]

3.116
practice guidelines
descriptive tools or standardized specification for care of the typical (subject of care) in the typical situation, developed through a formal process that incorporates the best scientific evidence of effectiveness with expert opinion

[JCAHO]

3.117
privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual

[ISO/IEC 2382-8]

right of individuals to keep information about themselves from being disclosed to anyone

[CPRI]

security principle that protects individuals from the collection, storage and dissemination of information about themselves and the possible compromises resulting from unauthorized release of that information

[HL7 Security SIG]

3.118
private key
key that is used with an asymmetric cryptographic algorithm and whose possession is restricted (usually to only one entity)

[ISO 10181-1]

NOTE This key may be used for encipherment, decipherment or signature generation.

3.119
process
collection of steps taking place in a prescribed manner and leading to the accomplishment of some result

[ISO/IEC 15414]

goal-directed, interrelated series of actions, events, mechanisms, or steps

[JCAHO]

3.120
protocol (care)
cf. **critical paths**

3.121
public key
key that is used with an asymmetric cryptographic algorithm and can be made publicly available

[ISO 10181-1]

NOTE This key may be used for encipherment, decipherment or signature verification.

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

3.122
public key certificate
X.509 public key certificates (PKCs) [X.509], binding an identity and a public key

[RFC2459, modified]

NOTE The identity may be used to support identity-based access control decisions after the client proves that it has access to the private key that corresponds to the public key contained in the PKC.

3.123
public key infrastructure
PKI
infrastructure used in the relation between a key holder and a relying party that allows a relying party to use a certificate relating to the key holder for at least one application using a public key dependent security service

NOTE PKI includes a Certification Authority, a certificate data structure, means for the relying party to obtain current information on the revocation status of the certificate, a certification policy and methods to validate the certification practice.

3.124
purpose (of a system)
practical advantage or intended effect of the system

[ISO/IEC 15414]

3.125
quality
totality of features and characteristics of a product, process or service that bear on its ability to satisfy its stated or intended needs

[CEN]

character, characteristic or property of anything that makes it good or bad, commendable or reprehensible; thus the degree of excellence that a thing possesses; totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs; fitness for use

[JCAHO]

3.126
quality improvement
approach to the continuous study and improvement of the processes of providing healthcare services to meet the needs of patients and others

[JCAHO]

3.127
recovery
restoration of an information system back to an error-free and secure state from which normal operation can resume

[CEN]

3.128
registry
server capable of holding data for the systematic and continuous follow up of information objects maintained in accordance with specific rules

3.129
release of information
disclosure of documents containing (subject of care)-identifiable information to a third party requestor

[CPRI]

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001

3.130
repudiation
denial by one of the entities involved in a communication of having participated in all or part of the communication

[ASTM E1762]

3.131
resource
enterprise object modelling an entity which is essential to some behaviour and which requires allocation or may become unavailable because it is in use or used up

[ISO/IEC 15414]

3.132
retention
maintenance and preservation of information in some form (e.g. paper, microfilm, or electronic storage) for a given period of time

[CPRI]

3.133
secondary record
record that is derived from the primary record and contains selected data elements

[ASTM E1384]

3.134
security
combination of availability, confidentiality, integrity and accountability

[CEN ENV 13608-1]

protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document and counter such threats

[NSC]

preservation of the confidentiality and integrity of data as well as ensuring the accountability and availability of data; combination of availability, confidentiality, integrity and accountability

[CEN ENV 12924, MEDSEC]

result of effective protection measures that safeguard data/information from undesired occurrences and exposure to accidental or intentional disclosure to unauthorized persons, accidental or malicious alteration, unauthorized copying, software deficiencies, operating mistakes, or sabotage

[IOM]

3.135
security (data)
protection of data from intentional or unintentional destruction, modification, or disclosure

[JCAHO]

3.136
security policy
plan or course of action adopted for providing computer security

[ISO/IEC 2382-8]

set of laws, rules, and practices that regulate how an organization manages, protects and distributes sensitive information

[DOD Orange Book]

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals; statement of information values, protection responsibilities and organization commitment for a system; set of laws, rules and practices that regulate how an organization manages, protects and distributes sensitive information

[OTA]

3.137
standard
document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context

[ISO/IEC Guide 2: 1996]

NOTE Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits.

3.138
step
task in a process

[ISO/IEC 15414]

3.139
subject of care
person or defined groups of persons receiving or registered as eligible to receive healthcare services or having received healthcare services

[CEN ENV 12443:1996]

NOTE For example, a patient, client, customer, or health plan member.

3.140
systematic
pursuing defined objective(s) in a planned, step-by-step manner

[JCAHO]

3.141
trust
confidence; a basis of reliance, faith, or hope; assured reliance on the character, strength, or truth of someone or something

[Merriam-Webster's Dictionary]

3.142
trusted system
system believed to enforce a given set of attributes to a stated degree of assurance (confidence)

[NRC]

system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information

[GCST]

4.143
use (of health information)
sharing, employment, application, utilization, examination, or analysis of such information

[HIPAA]

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001

3.144
user
person or other entity authorized by a provider to use some or all of the services provided by the provider

[COACH]

human being using the system to issue requests to objects in order to get them to perform functions in the system on his/her behalf

[OMG]

4 Abbreviated terms

AHA	American Hospital Association
ANSI	American National Standards Institute
API	Application Program Interface
ASC X12	Accredited Standards Committee X12, an ANSI Accredited SDO
ASTM E31	American Society for Testing Materials, Committee E31 on Healthcare Informatics
DICOM	Digital Imaging and Communications in Medicine; standard developed by NEMA
CCITT	Consultative Committee on International Telephony and Telegraphy
CEN	Comité Européen de Normalisation, European Committee for Normalization
CIHI	Canadian Institute for Health Information
COACH	Canadian Organisation for the Advancement of Computers in Health (now Canadian Health Informatics Association)
CPRI	Computer-Based Patient Record Institute
DOD	U.S. Department of Defense
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport (also referred to as UN/EDIFACT)
EHR, EHCR	electronic health record, electronic healthcare record
ENV	CEN European Pre-Standard
GCST	US DOD Glossary of Computer Security Terms
HCFA	US DHHS Healthcare Financing Administration
HIPAA	Health Insurance Portability and Accountability Act of 1996, US Public Law 104-191
HISB	ANSI Healthcare Informatics Standards Board
HL7	Health Level Seven, an ANSI Accredited SDO
HMO	Health Management Organization
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IOM	Institute of Medicine, a body of the US National Institutes of Health

Documents
Document Sharing Hub

Full document details: PD ISO/TR 18307:2001

ISO	International Organization for Standardization
ISO TC215	ISO Technical Committee 215 on Healthcare Informatics
ITSEC	Information Technology Security Evaluation Criteria
JCAHO	Joint Commission for Accreditation of Healthcare Organizations
KC	Key Characteristic(s), the primary topic of this ISO Technical Report
MEDSEC	Healthcare Security and Privacy in the Information Society, project sponsored by the European Commission
MIB	IEEE Committee P1073, Medical Information Bus
NCQA	National Council for Quality Assurance (US)
NCVHS	U.S. DHHS National Council for Vital and Health Statistics
NEHRT	National Electronic Health Records Taskforce (Australia)
NEMA	National Electrical Manufacturers Association
NHS	National Health Service (UK)
NIST	National Institute for Standards and Technology (US)
NMB	ISO National Member Body
NRC	National Research Council (US)
NSC	National Security Council (US)
ODP	Open Distributed Processing
OLAP	On-Line Analytical Processing
OLTP	On-Line Transaction Processing
OMG	Object Management Group
OTA	Office of Technology Assessment (US)
PKC	Public Key Certificate
PKI	Public Key Infrastructure
RM-ODP	Reference Model for Open Distributed Processing
SDO	Standards Developing Organization
SIG	Special Interest Group
TR	ISO Technical Report
USHIK	U.S. Health Information KnowledgeBase, a data registry maintained by the U.S. DHHS (HCFA) and DOD
UN	United Nations
WEDI	Work Group for Electronic Data Interchange
WG2	ISO TC215, Working Group 2 on Messaging and Communications

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001

5 Trust Constituency

The Trust Constituency consists of individuals, organizations and business units. The Trust Constituency relies substantially on ISO/TC 215 and its work products to protect and engage their rights and obligations with regard to health information interchange.

Table 1 identifies parties to the Trust Constituency.

Trust Constituency: for health record content, including individually identifiable information Constituent	Individual	Organization	Business unit	Subject of record	Accountable source, Author of record content	Accountable verifier of record content	Accountable scribe of record content	Accountable user of record content	Accountable record steward	Accountable provider of health services as documented in record
Subject of care, Health plan member	X			Yes	Yes	AA [b]	NA [a]	AA	No	No
Next of kin, Emergency contact	X			Yes	No	No	No	No	No	No
Healthcare professional, Caregiver	X			Yes	Yes	Yes	Yes	Yes	Yes	Yes
Care assistant	X			Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transcriptionist	X			Yes	No	AA	Yes	AA	Yes	No
Department, Service, Speciality			X	Yes	NA	NA	NA	Yes	Yes	Yes
Healthcare provider	X	X		Yes	NA	NA	NA	Yes	Yes	Yes
Integrated delivery network (IDN)		X		Yes	NA	NA	NA	Yes	Yes	Yes
Payment guarantor, Health plan, HMO	X	X		AA	No	No	No	Yes	Yes	No
Value added network, Claims clearinghouse		X		No	No	No	No	Yes	Yes	No
Employer	X	X		AA	No	No	No	Yes	AA	No
Public health agency		X		No	No	No	No	Yes	AA	No
Regulatory agency		X		No	No	No	No	Yes	AA	No
Accreditation agency		X		No	No	No	No	Yes	AA	No
Research	X	X		No	No	No	No	Yes	AA	No
Professional education	X	X		No	No	No	No	Yes	AA	No
Others										

[a] Not applicable.
[b] As applicable.

Table 1 — The Trust Constituency (for health records and record interchange)

Documents
Document Sharing Hub
Full document details: PD ISO/TR 18307:2001